PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-171863
(43)Date of publication of application : 26.06.1998

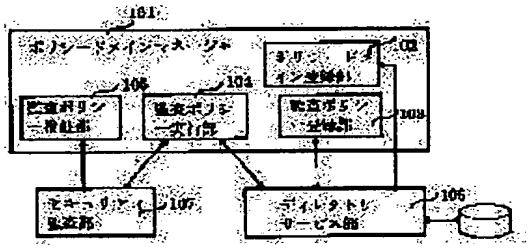
(51)Int.Cl. G06F 17/60

(21)Application number : 08-325051
(22)Date of filing : 05.12.1996

(71)Applicant : HITACHI LTD
(72)Inventor : NISHIKI KENYA
HIRATA TOSHIAKI
MIYAZAKI SATOSHI

(54) SECURITY AUDIT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security audit system which is coherent in the entire organization can be obtained, and an audit policy which can be flexibly set according to an organization constitution can be executed.
SOLUTION: This system is provided with a policy domain registering part 102 which registers the execution range of an audit policy indicating the executing method of audit in a directory service part 106, audit policy registering part 103 which registers the audit policy in the directory service part 106, audit policy executing part 104 which sets the registered audit policy in a security audit part 107, and audit policy verifying part 105 which operates the coherence check of the audit policy based on the audit result information of th security audit part 107.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the xaminer's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of xtinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－171863

(43)公開日　平成10年(1998)６月26日

(51)Int.Cl.[6]　識別記号　ＦＩ

G06F 17/60　G06F 15/21　Z

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願平8－325051

(22)出願日　平成８年(1996)12月５日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　西木　健哉
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　平田　俊明
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　宮崎　聡
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

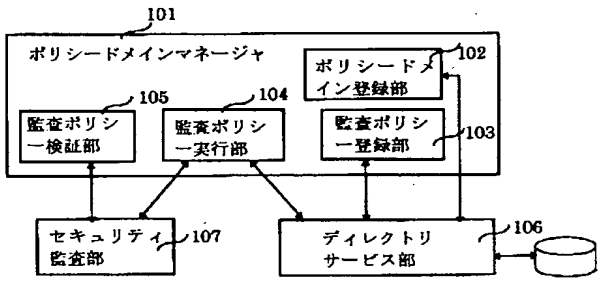
(54)【発明の名称】セキュリティ監査システム

(57)【要約】

【課題】セキュリティの監査ポリシーをマシン個別あるいは管理するドメイン個別に設定しなければならない手間と、複数の管理者によって管理される場合に監査レベルにばらつきが生じる。

【解決手段】監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部１０６に登録するポリシードメイン登録部１０２と、監査ポリシーをディレクトリサービス部１０６に登録する監査ポリシー登録部１０３と、登録された監査ポリシーをセキュリティ監査部１０７に設定する監査ポリシー実行部１０４と、セキュリティ監査部１０７の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証部１０５でなる。

図１



1

【特許請求の範囲】

【請求項１】通信ネットワークによって複数のコンピュータシステムが接続されたインター／イントラネット環境で、ネットワーク資源を論理的な依存関係や包含関係に基づいて階層的に構成しユーザからネットワーク資源へのアクセスを管理するディレクトリサービス部と、ネットワーク資源へのユーザアクセスに関する情報をリアルタイムに収集し記録したり、コンピュータシステム上にインストールされたプログラムの正当性および安全性を確認するセキュリティ監査部とを備えたセキュリティ監査システムにおいて、

監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部に登録するポリシードメイン登録手段と、監査ポリシーをディレクトリサービス部に登録する監査ポリシー登録手段と、登録された監査ポリシーを前記セキュリティ監査部に設定する監査ポリシー実行手段と、セキュリティ監査部の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証手段とを有することを特徴とするセキュリティ監査システム。

【請求項２】請求項１において、前記ポリシードメイン登録手段は、前記監査ポリシー登録手段、監査ポリシー実行手段および監査ポリシー検証手段を実行する主体である監査ポリシーマネージャを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、監査ポリシーマネージャーが監査の対象とするオブジェクト名を属性とする被監査オブジェクトを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、前記監査ポリシーマネージャオブジェクトおよび被監査オブジェクトで構成されるポリシードメインを、前記ディレクトリサービス部の上位階層のオブジェクトとして登録する手段とを有するセキュリティ監査システム。

【請求項３】請求項１において、前記監査ポリシー登録手段は、監査対象のオブジェクト種別、監査の有無、監査する項目、監査の行使スケジュール、監査の報告方法に関する属性の入力を受け付けて、前記ディレクトリサービス部の当該監査ポリシーの行使されるポリシードメインオブジェクトの配下のオブジェクトとして登録する手段を有し、前記監査ポリシー実行手段は、前記ディレクトリサービス部の該当する監査ポリシーオブジェクトの属性を取得し、これを監査対象オブジェクトに設定する手段を有するセキュリティ監査システム。

【請求項４】請求項１において、前記監査ポリシー登録手段は、ポリシーオブジェクトがそれが属するポリシードメインの下位のポリシードメインにデフォルトのポリシーオブジェクトとして継承させることの有無を表す属性とポリシー属性の変更を許可することの可否を表す属性の入力を受け付けて、当該オブジェクトに設定する手段を有し、前記ポリシードメイン登録手段は、ポリシードメインをすでに登録されたポリシードメインオブジェクトの下位オブジェクトとして登録する手段と、上位のポリシードメインに含まれるポリシーオブジェクトが継承属性を持つ場合に当該ポリシーオブジェクトの複製を作成し、ポリシーの変更属性にあわせてオブジェクトのアクセス権を設定する手段とを有するセキュリティ監査システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークシステムにおけるセキュリティ監査システムに関するものである。

【０００２】

【従来の技術】ネットワーク資源に対する内部あるいは外部からの不正なアクセスに対処するために通常のＯＳはユーザ認証機構やファイルなどへのアクセス制御機構を備えている。さらにネットワークシステムレベルでのユーザ認証やアクセス制御を実現する技術としてディレクトリサービスと呼ばれる技術が知られており、これによってネットワーク資源を論理的なオブジェクトの階層関係に基づいて一元的に管理することができる。このようなディレクトリサービスについては、“NetWare４．１Ｊディレクトリサービスの概要”；Novellなどに記載されている。

【０００３】またネットワーク資源へのアクセスを逐次ログファイルに登録する監査機構が知られており、このような監査機構については、“WindowsＮＴ３．５セキュリティ／監査ガイド”；ＡＳＣＩＩなどに記載されている。

【０００４】

【発明が解決しようとする課題】さて、企業などの組織でセキュリティを確保する場合には、セキュリティに関する標準規約を決め組織全体で一貫性のあるものとしなければならない。組織の一部にセキュリティの穴があれば、そこからの不正侵入が組織全体に広がるおそれがある。このような従来技術では、セキュリティの監査ポリシーをマシン個別あるいは管理するドメイン個別に設定しなければならないという手間と、管理者がたとえば部署単位に複数存在する場合には監査レベルにばらつきが生じてしまう問題がある。また監査ポリシーが遵守されているかどうかをチェックする仕掛けも提供されていない。

【０００５】本発明の目的は、組織全体で一貫性があり、かつ組織構成に応じて柔軟に設定可能な監査ポリシーを実施することのできるセキュリティ監査システムを提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明は、ネットワーク資源を論理的な依存関係や包含関係に基づいて階層的に構成しユーザからネットワーク資源へのアクセスを管理するディレクトリサービス

部と、ネットワーク資源へのユーザアクセスに関する情報をリアルタイムに収集し記録したり、コンピュータシステム上にインストールされたプログラムの正当性および安全性を確認するセキュリティ監査部とを備えたセキュリティ監査システムにおいて、監査の実施方法を表す監査ポリシーの行使範囲をディレクトリサービス部に登録するポリシードメイン登録手段と、監査ポリシーをディレクトリサービス部に登録する監査ポリシー登録手段と、登録された監査ポリシーを前記セキュリティ監査部に設定する監査ポリシー実行手段と、セキュリティ監査部の監査結果情報に基づいて監査ポリシーの一貫性チェックを行う監査ポリシー検証手段とを有するセキュリティ監査システムを提供する。

【０００７】また前記ポリシードメイン登録手段は、前記監査ポリシー登録手段、監査ポリシー実行手段および監査ポリシー検証手段を実行する主体である監査ポリシーマネージャを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、監査ポリシーマネージャが監査の対象とするオブジェクト名を属性とする被監査オブジェクトを、前記ディレクトリサービス部のオブジェクトとして登録する手段と、前記監査ポリシーマネージャオブジェクトおよび被監査オブジェクトで構成されるポリシードメインを、前記ディレクトリサービス部の上位階層のオブジェクトとして登録する手段とを有するセキュリティ監査システムを提供する。

【０００８】また前記監査ポリシー登録手段は、監査対象のオブジェクト種別、監査の有無、監査する項目、監査の行使スケジュール、監査の報告方法に関する属性の入力を受け付けて、前記ディレクトリサービス部の当該監査ポリシーの行使されるポリシードメインオブジェクトの配下のオブジェクトとして登録する手段を有し、前記監査ポリシー実行手段は、前記ディレクトリサービス部の該当する監査ポリシーオブジェクトの属性を取得し、これを監査対象オブジェクトに設定する手段を有するセキュリティ監査システムを提供する。

【０００９】また前記監査ポリシー登録手段は、ポリシーオブジェクトがそれが属するポリシードメインの下位のポリシードメインにデフォルトのポリシーオブジェクトとして継承させることの有無を表す属性とポリシー属性の変更を許可することの可否を表す属性の入力を受け付けて、当該オブジェクトに設定する手段を有し、前記ポリシードメイン登録手段は、ポリシードメインをすでに登録されたポリシードメインオブジェクトの下位オブジェクトとして登録する手段と、上位のポリシードメインに含まれるポリシーオブジェクトが継承属性を持つ場合に当該ポリシーオブジェクトの複製を作成し、さらにポリシーの変更属性にあわせてオブジェクトのアクセス権を設定する手段とを有するセキュリティ監査システムを提供する。

【００１０】このようなセキュリティ監査システムによれば、監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているので、複数の管理者によって分散管理されているシステムにおいても一貫性が保証される。またディレクトリサービスの階層関係を利用して階層化された監査ポリシーを実施でき、柔軟にセキュリティレベルを変更することが可能である。

【００１１】

【発明の実施の形態】本発明の第一の実施例を図１に示すセキュリティ監査システムのブロック図を用いて説明する。

【００１２】ポリシードメインマネージャ１０１は、ポリシードメイン単位に監査ポリシーを実行する主体であり、ポリシードメイン登録部１０２、監査ポリシー登録部１０３、監査ポリシー実行部１０４、監査ポリシー検証部１０５で構成される。ポリシードメイン登録部１０２、監査ポリシー登録部１０３、監査ポリシー実行部１０４はディレクトリサービス部１０６にアクセスすることができる。また、監査ポリシー実行部１０４、監査ポリシー検証部１０５はセキュリティ監査部１０７にアクセスすることができる。

【００１３】また図１に示したセキュリティ監査システムは、たとえば図２に示すような、入力装置２０４、表示装置２０５、ＣＰＵ２０２、メモリ２０３、記憶装置２０６などのハードウェアを備えた電子計算機上に構築することができる。この場合、ポリシードメイン登録部１０２、監査ポリシー登録部１０３、監査ポリシー実行部１０４、監査ポリシー検証部１０５、ディレクトリサービス部１０６、セキュリティ監査部１０７は電子計算機上で実行されるプロセスとして具体化される。

【００１４】ディレクトリサービス部１０６は、たとえばネットワーク・オーエス（ＮＯＳ）の提供するディレクトリサービスによって実現することができ、ディレクトリ内のオブジェクトは分散データベースのデータとして管理される。またセキュリティ監査部１０７は監査対象である各電子計算機のオーエス（ＯＳ）が提供する監査インターフェースを使用して実現することができる。

【００１５】図３のネットワークシステム構成図を用いて、監査ポリシーを実施する全体フローを説明する。図３ではポリシードメインとしてセンタードメイン３０１と営業店ドメイン３０２が存在する。まずセンタードメイン３０１においてポリシードメインマネージャであるＰＤＭ３０３のポリシードメイン登録処理部で前記２つのポリシードメインをディレクトリサービス部であるＤＳ３０４に登録する。このとき営業店ドメインオブジェクトはセンタドメインオブジェクトの下位に位置するオブジェクトとして登録する。

【００１６】次にＰＤＭ－１の監査ポリシー登録部がたとえばサーバの監査を行うための監査ポリシーをディレクトリサービス部ＤＳ－１に登録する。ＰＤＭ３０３の

監査ポリシー実行部はＤＳ－１に登録されている監査ポリシーをセンタードメイン内のサーバオブジェクトであるサーバ３０５、サーバ３０６などに対して設定する。さらにＤＳ３０４に登録されたポリシードメインオブジェクトおよび監査ポリシーオブジェクトはディレクトリサービスの提供するディレクトリ同期処理によって営業店ドメイン内のディレクトリサービス部ＤＳ３０７の参照するデータベースに反映される。営業店ドメインのポリシードメインマネージャであるＰＤＭ３０８の監査ポリシー実行部はセンタードメインで設定されたサーバに関する監査ポリシーを継承し、営業店ドメイン内のサーバオブジェクトであるサーバ３０９、サーバ３１０などに対して設定する。またＰＤＭ３０８の監査ポリシー登録部はＰＤＭ３０３で登録された監査ポリシーとは別の監査ポリシーを登録し、実行することも可能である。

【００１７】またＰＤＭ３０３の監査ポリシー検証部は、監査ポリシーの登録および実行処理とは独立に管理者の指示したタイミングで実行される。

【００１８】次に図４のフローチャートを用いてポリシードメイン登録処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサービス部に接続する（４０１）。既存ドメインが登録されている場合には新規ドメインと既存ドメインとの間に継承関係を設定するかどうかを選択させ（４０２）、継承関係を設定する場合には既存ドメインの上位あるいは下位にドメインオブジェクトを登録する（４０３）。オブジェクトはディレクトリサービス部によって管理可能なたとえば図８～図１０の形式で格納する。

【００１９】図８に示すディレクトリオブジェクト構成テーブル８００は、対応するオブジェクトを識別するためのオブジェクト識別子８０１、オブジェクトの階層構造上の位置を示すオブジェクト位置識別子８０２、ネットワーク資源の種別を示すオブジェクトタイプ８０３、アクセス権利テーブルへのポインタ８０４、オブジェクトプロパティテーブルへのポインタ８０５、および次のテーブルエントリへのポインタ８０６からなる。図９に示すアクセス権利テーブル９００は、オブジェクトへのアクセス権利を保有するオブジェクト識別名９０１、オブジェクトアクセスもしくはプロパティアクセスを示すアクセスタイプ９０２、およびオブジェクトに記憶された情報の参照、更新などの内容を示すアクセス権利９０３からなる。図１０に示すオブジェクトプロパティテーブル１０００は、プロパティ１００１、プロパティ値１００２、および次のテーブルエントリへのポインタ１００３からなる。

【００２０】次に図５のフローチャートを用いて監査ポリシー登録処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサービス部に接続し（５０１）、登録されたポリシードメインのなかから監査ポリシーを作成するポリシードメインを選択する。この場合、ポリシードメインマネージャは選択したポリシードメインオブジェクトに対する適切なアクセス権を保有している必要がある。次に監査対象のオブジェクト種別、監査の有無、監査する項目（たとえばログオン／ログオフ、ファイルアクセス、ユーザとグループの設定、システム再起動などについての成功あるいは失敗）、監査の行使スケジュール、監査の報告方法（たとえばログファイルに登録する、指定されたユーザにメッセージを送信など）をそれぞれプロパティとして持つ監査ポリシーオブジェクトとして、ドメインオブジェクトの配下に登録する（５０３）。既存の監査ポリシーを選択して特定のプロパティを変更することも可能である。次に登録された監査ポリシーを下位のポリシードメインに継承させるかどうかを選択し（５０４）、継承させる場合には継承属性をオブジェクトに付加する（５０５）。さらに継承された監査ポリシーの変更を許可するかどうかを選択し（５０６）、変更を許可する場合には変更可能属性をオブジェクトに付加する（５０７）。

【００２１】次に図６のフローチャートを用いて監査ポリシー実行処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサーバに接続し（６０１）、ポリシードメインマネージャの管理する監査対象オブジェクトの情報および監査ポリシー情報を取得する（６０２）。監査ポリシーのオブジェクト種別にあてはまる監査対象オブジェクトについてオブジェクトを管理するセキュリティ監査部にアクセスして、監査ポリシーの内容を設定する（６０３）。

【００２２】次に図７のフローチャートを用いて監査ポリシー検証処理の詳細を説明する。まずポリシードメインマネージャの属するディレクトリサーバに接続し（７０１）、監査ポリシー情報を取得し、現在監査対象となっているオブジェクトを特定する（７０２）。次にオブジェクトを管理するセキュリティ監査部にアクセスし、監査結果情報（たとえばセキュリティログファイル）を取得し（７０３）、監査ポリシーに従って監査が行われているかどうかをチェックする（７０４）。チェックは管理者の判断で行うケースとチェックプログラムを使用して行うケースにわかれる。またポリシードメインの配下にポリシードメインが存在する場合には（７０５）、配下ポリシードメインマネージャを起動して監査ポリシーの検証を行う（７０６）。配下のドメインに監査ポリシーを継承させており、かつ監査ポリシーの変更を許可していない場合には上位の監査ポリシーに照らして検証を行う。監査ポリシー違反が検出された場合にはポリシードメインの管理者に特定のアラーをあげることによってこれを通知する。

【００２３】本実施例のセキュリティ監査システムによれば、監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているので、複数の管理者によって分散管理されているシステムにお

いても一貫性が保証される。ディレクトリサービスの階層関係を利用して階層化された監査ポリシーを実施でき、柔軟にセキュリティレベルを変更することが可能である。

【００２４】

【発明の効果】本発明では、ポリシードメイン登録手段によってセキュリティレベルに対応した階層的な管理ドメインを構築でき、監査ポリシー登録、実行、検証手段によって監査ポリシーを分散型のデータベース機構を備えるディレクトリサービスを利用して管理しているので、複数の管理者によって分散管理されているシステムにおいても監査ポリシーへのアクセス制御が実現できる。またポリシードメイン間で監視ポリシーを継承させることによって監視ポリシーの設定の手間を軽減できるとともにシステム全体での監視ポリシーの一貫性を確保できる。

【図面の簡単な説明】

【図１】本発明の実施例のシステムのブロック図。

【図２】本発明の実施例のシステムのハードウェアのブロック図。

【図３】本発明の実施例のセキュリティ監査システムのブロック図。

【図４】本発明の実施例のポリシードメインの登録のフローチャート。

【図５】本発明の実施例の監査ポリシーの登録のフローチャート。

【図６】本発明の実施例の監査ポリシーの実行のフローチャート。

【図７】本発明の実施例の監査ポリシーの検証のフローチャート。

【図８】本発明の実施例のディレクトリオブジェクトテーブルの形式を示す説明図。

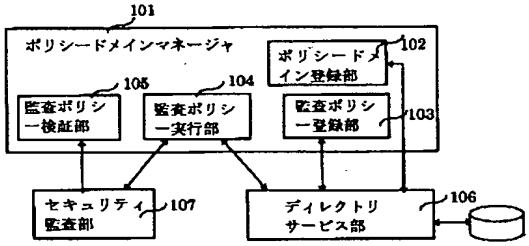
【図９】本発明の実施例のアクセス権利エントリの形式を示す説明図。

【図１０】本発明の実施例のオブジェクトプロパティテーブルの形式を示す説明図。

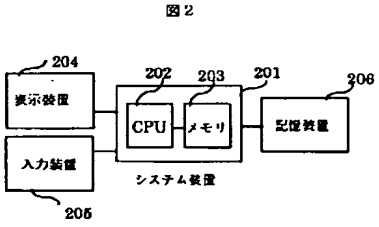
【符号の説明】

１０１…ポリシードメインマネージャ、
１０２…ポリシードメイン登録部、
１０３…監査ポリシー登録部、
１０４…監査ポリシー実行部、
１０５…監査ポリシー検証部、
１０６…ディレクトリサービス部、
１０７…セキュリティ監査部。

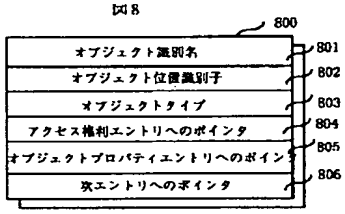
【図１】



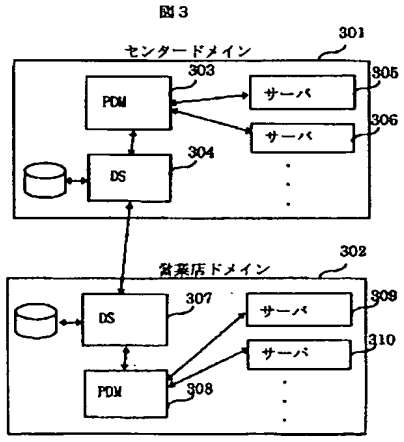
【図２】



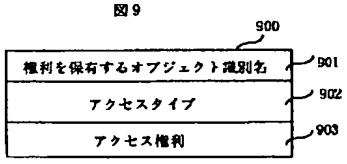
【図８】



【図３】

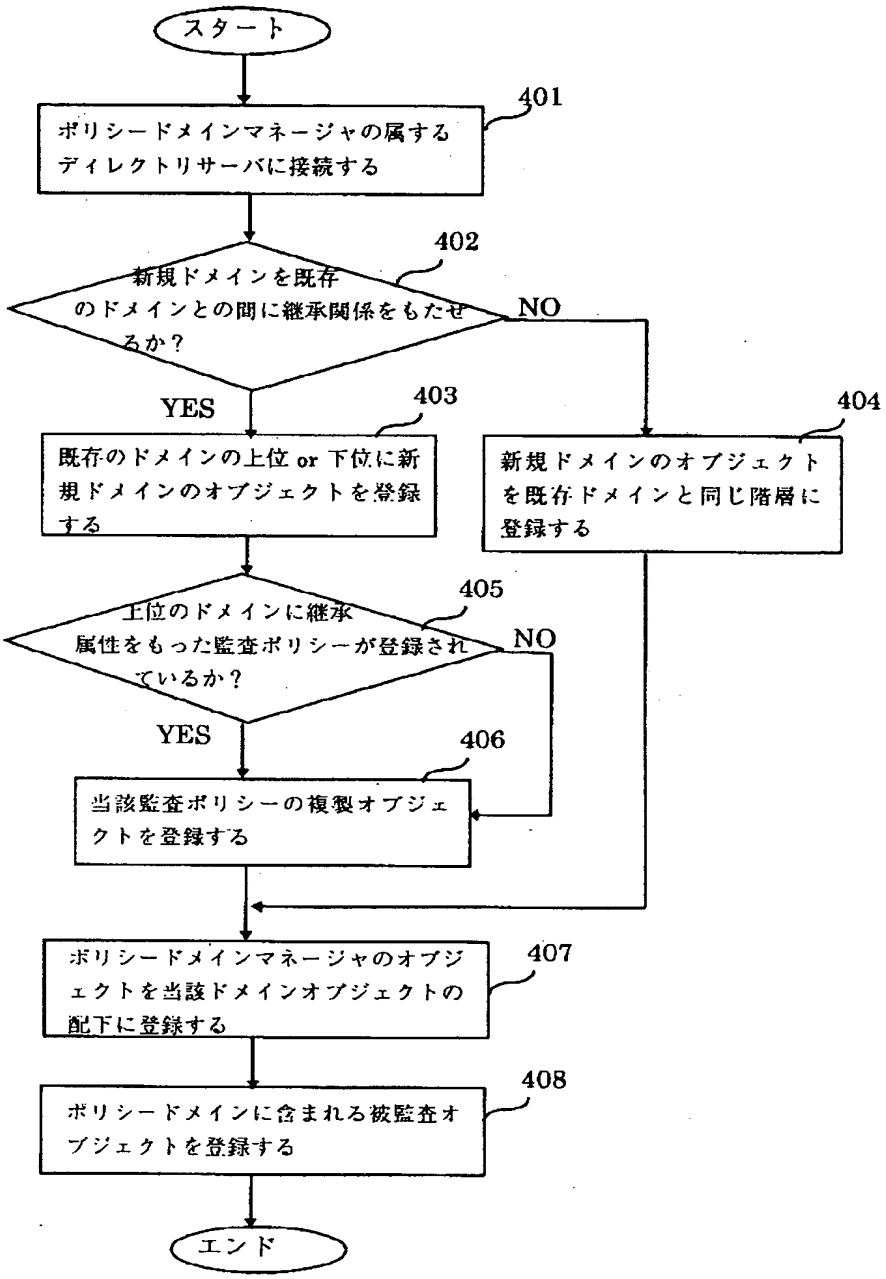


【図９】



【図４】

図４


スタート
401
ポリシードメインマネージャの属するディレクトリサーバに接続する
402
新規ドメインを既存のドメインとの間に継承関係をもたせるか？
NO
YES
403
既存のドメインの上位 or 下位に新規ドメインのオブジェクトを登録する
404
新規ドメインのオブジェクトを既存ドメインと同じ階層に登録する
405
上位のドメインに継承属性をもった監査ポリシーが登録されているか？
NO
YES
406
当該監査ポリシーの複製オブジェクトを登録する
ポリシードメインマネージャのオブジェクトを当該ドメインオブジェクトの配下に登録する
407
408
ポリシードメインに含まれる被監査オブジェクトを登録する
エンド

【図１０】

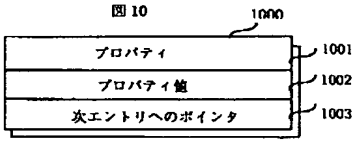
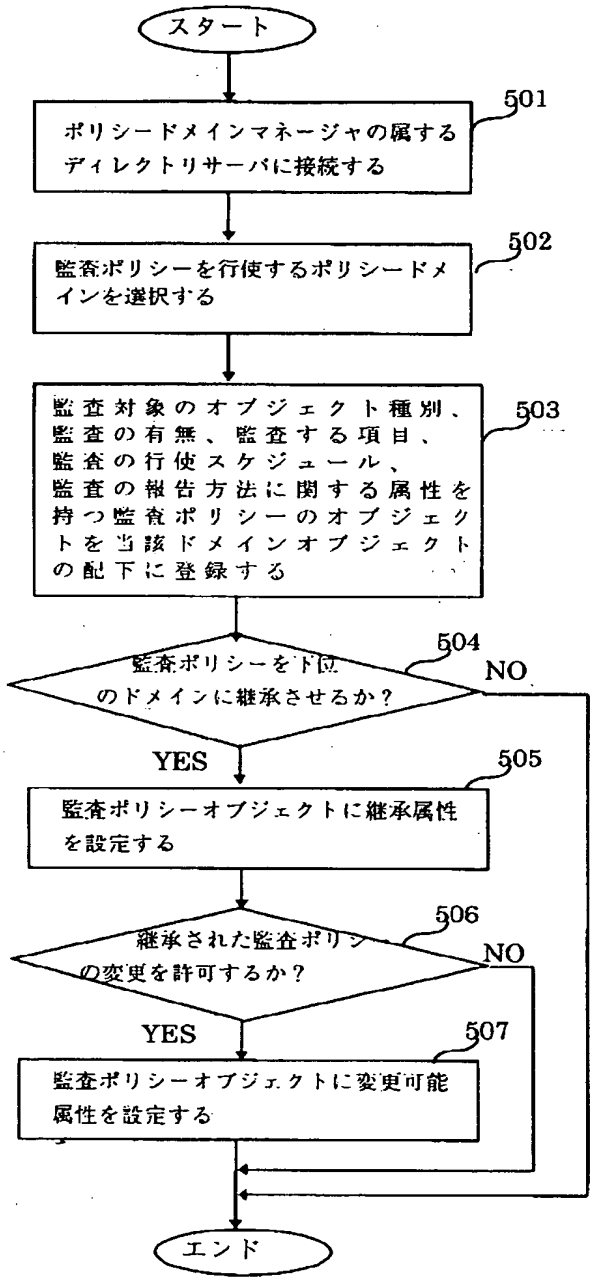


図 10
1000
プロパティ
1001
プロパティ値
1002
次エントリへのポインタ
1003

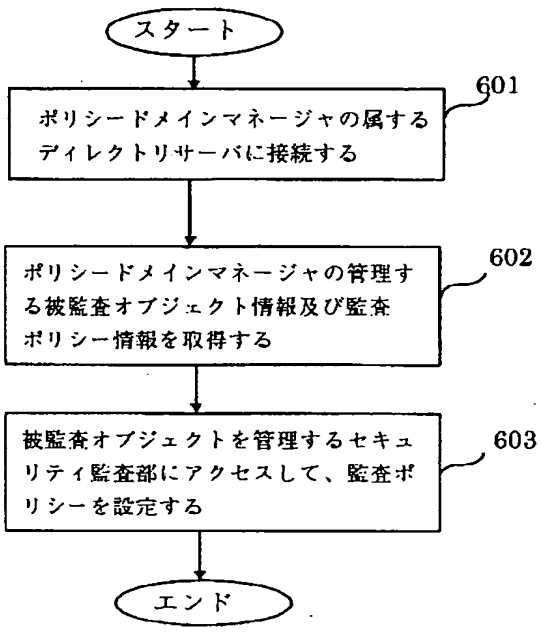
【図５】

図５


スタート
ポリシードメインマネージャの属するディレクトリサーバに接続する
501
監査ポリシーを行使するポリシードメインを選択する
502
監査対象のオブジェクト種別、監査の有無、監査する項目、監査の行使スケジュール、監査の報告方法に関する属性を持つ監査ポリシーのオブジェクトを当該ドメインオブジェクトの配下に登録する
503
監査ポリシーを下位のドメインに継承させるか？
504
NO
YES
監査ポリシーオブジェクトに継承属性を設定する
505
継承された監査ポリシーの変更を許可するか？
506
NO
YES
監査ポリシーオブジェクトに変更可能属性を設定する
507
エンド

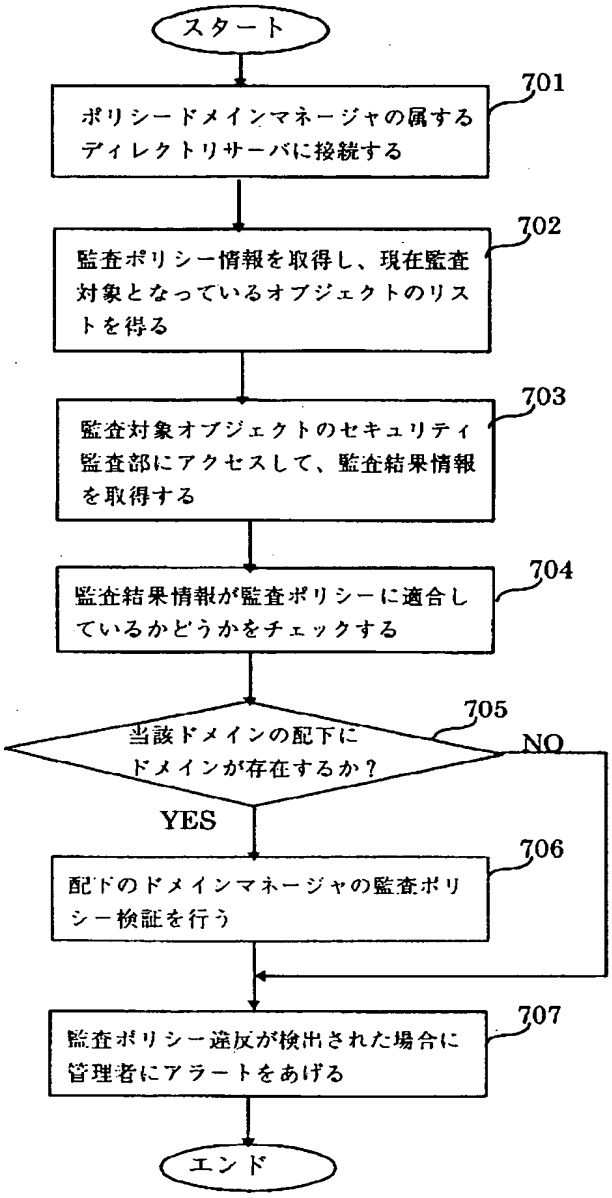
【図６】

図６


スタート
ポリシードメインマネージャの属するディレクトリサーバに接続する
601
ポリシードメインマネージャの管理する被監査オブジェクト情報及び監査ポリシー情報を取得する
602
被監査オブジェクトを管理するセキュリティ監査部にアクセスして、監査ポリシーを設定する
603
エンド

【図７】

図７


スタート
701
ポリシードメインマネージャの属するディレクトリサーバに接続する
702
監査ポリシー情報を取得し、現在監査対象となっているオブジェクトのリストを得る
703
監査対象オブジェクトのセキュリティ監査部にアクセスして、監査結果情報を取得する
704
監査結果情報が監査ポリシーに適合しているかどうかをチェックする
705
当該ドメインの配下にドメインが存在するか？
NO
YES
706
配下のドメインマネージャの監査ポリシー検証を行う
707
監査ポリシー違反が検出された場合に管理者にアラートをあげる
エンド